Allowance

Claims **1 - 3, 5 - 36** are pending.

Terminal Disclaimer

The terminal disclaimers filed on 3-30-2010 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of *copending applications* 10/690,422; 10/849,090; 10/994,010 have been reviewed and is accepted. The terminal disclaimers have been recorded.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Bryan Webster at 425-538-2731/ bweb@microsoft.com on 3-9-2010.

Amended Claims are 1, 13, 24, 31, 32, 36:

1. (Currently Amended) A hardware-implemented computer system for processing e-mail comprising:

a memory;

a plurality of servers that receive e-mail messages from a plurality of remotely located clients, the plurality of servers being part of a distributed network;

a plurality of packet sniffers, wherein each of the packet sniffers in the plurality of packet sniffers corresponds to and resides in a different server in the plurality of servers, wherein each packet sniffer in the plurality of packet sniffers is configured to; a) check a fragment offset field of an IP header to ensure the IP header is the first fragment of a packet, b)determine the value of a SYN bit in a TCP header, c) disregarding the packet if the SYN bit has not been set, and if the frame does not include an IP address, and if the IP address does not correspond to the server on which the packet sniffer is running, and if the IP address does not correspond to the configured port number and d)extract from the received packet originating IP addresses associated with e-mail messages that are communicated to the clients over the distributed network;

a central monitor that communicates over the distributed network with the plurality of packet sniffers and that monitors data regarding the originating IP addresses, wherein the central monitor is configured to determine whether traffic from an originating IP address has exceeded a threshold value, the central monitor being further configured to generate a response to detect spam e-mail messages if the threshold value has been exceeded; and

13. (Currently Amended) A hardware-implemented system for detecting spam e-mail messages in a distributed network including a plurality of servers that receive and process e-mail messages for a plurality of different remotely located clients, the system comprising:

a memory;

a plurality of packet sniffers, each of which is located on a unique one of the plurality of servers, such that each of a plurality of packet sniffers are configured to; a)check a fragment offset field of an IP header to ensure the IP header is the first fragment of a packet, b) determine the value of a SYN bit in a TCP header, c) disregarding the packet if the SYN bit has not been set, and if the frame does not

include an IP address, and if the IP address does not correspond to the server on which the packet sniffer is running, and if the IP address does not correspond to the configured port number and d) extract originating IP addresses associated with e-mail messages that are communicated to clients by the server;

a central monitor that communicates with the plurality of packet sniffers and that monitors data regarding the originating IP addresses, wherein the central monitor is configured to determine whether traffic from an originating IP address has exceeded a threshold value, the central monitor being further configured to generate a response to detect spam e-mail messages if the threshold value has been exceeded; and

a server in which the central monitor resides, wherein the server is distinct from each of the packet sniffers in the plurality of packet sniffers in the distributed network.

24. (Currently Amended) A method for processing e-mail and detecting spam e-mail messages, comprising:

routing the e-mail messages of a computer through a distributed network including a plurality of servers that receive and process e-mail messages for a plurality of different remotely located clients;

communicating the processed messages to the plurality of remotely located clients by use of the plurality of servers;

a) checking a fragment offset field of an IP header to ensure the IP header is the first fragment of a packet, b) determining the value of a SYN bit in a TCP header, c) disregarding the packet if the SYN bit has not been set, and if the frame does not include an IP address, and if the IP address does not correspond to the server on which the packet sniffer is running, and if the IP address does not correspond to the configured port number and d) extracting, at the plurality of servers, originating IP addresses associated with e-mail messages that are communicated to the plurality of remotely located clients;

monitoring data regarding originating IP addresses;

determining whether traffic from an originating IP address has exceeded a threshold value; and

generating, at a central monitor, a response for use in detecting spam e-mail messages if the threshold value has been exceeded.

31. (Currently Amended) The ~~system~~ method of claim 30 wherein the response generated by the central monitor comprises a command to add the originating IP address to the blacklist.

32. (Currently Amended) The method[[']] of claim 24 further comprising:

storing rules for determining whether e-mail messages are spam in a spam database; and

determining whether e-mail messages are spam based on the rules within the spam database.

36. (Currently Amended) The ~~system~~ method of claim 24 wherein the response generated by the central monitor comprises a command to the system to block future e-mail messages from the originating IP address.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance:

Claims **1, 13, 24** are allowed based on the following:

The prior art of record, considered individually or in combination, fails to fairly show or suggest: disregarding the packet if the SYN bit has not been set, and if the frame does not include an IP address, and if the IP address does not correspond to the server on which the packet sniffer is running, and if the IP address does not correspond to the

configured port number and extract from the received packet originating IP addresses associated with e-mail messages that are communicated to the clients over the distributed network, in addition to the other limitations in a manner as recited in claims **1 - 3, 5 - 36**.

Claims **2, 3, 5 - 12** are allowed due to allowed base claim **1**.

Claims **14 - 23** are allowed due to allowed base claim **13**.

Claims **25 - 36** are allowed due to allowed base claim **24**.

So as indicated by the above statements, Applicant's arguments have been considered persuasive, in light of the set of claims with limitations as well as the enabling portions of the specification. The dependent claims further limit the independent claims and are considered allowable on the same basis as the independent claims as well as for the further limitations set forth.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung Hye Shin whose telephone number is (571) 272-3920. The examiner can normally be reached on 9:30 am - 6 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tonia L. Dollinger can be reached on (571) 272-4170. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

4-10-2010

/Kyung Hye Shin/
Examiner, Art Unit 2443